Finn Sparks

Dr. Ruoti

COSC 583

25 October 2025

Report On SSL Labs TLS

This report evaluates the outputs of Qualys SSL Labs to analyze ten websites' TLS usage and configurations. The data below details the specific configurations and properties for each website. This document was peer-reviewed by Tyler Hall.

The first detail of note is that almost all of the sites here support TLS 1.3. This allows for the best performance and security features, and this is seen even on some sketchier shopping websites (like Temu). Another similarity is that every secure site on the list uses RSA-2048 certificates, though some also have the ability to use Elliptic Curve keys in addition to RSA-2048 (Discord and Apple). All of the sites listed are also backed by public and trusted Certificate Authorities (CAs), which makes sense because a user would be warned and turned away from a site if this were not the case.

Although many of the sites have similar practices, some have distinct choices that set them apart. One of these is the use of HSTS (HTTP Strict Transport Security), which is not enforced consistently. Apple does not have it, but Temu does, which feels backwards. One website of note, Tata-Daewoo, is not a regular site but was included as one of the worst websites for TLS practices. It was added as a counter-example. It has many poor security configurations and is the only one that supports RC4 and 3DES, both of which have been proven insecure and are not recommended for use.

One of the biggest questions I have is about TLS 1.0 and 1.1. How insecure are they to have them even as options? Would it not be important to allow that for servers to communicate with legacy devices? Is the risk of supporting older protocols worse than blocking some users from accessing the site? Another question I have concerns Eastman: how is the second certificate in their chain also issued to themselves?

All in all, I feel like I learned a great deal from this assignment, and I'm pleased with the result!

Subject / CN / Alt Names	Validity Period	Key Type	Certificate Chain	Auth Algorithm	Symmetric Encryption / Key Size / Mode	Hashing Algorithm	Crypto Guarantees (CIA)	Three Interesting Notes
Subject: cluster95.canvas-user-content.com **CN:** cluster95.canvas-user-content.com **SANs:** cluster95.canvas-user-content.com, *.instructure.com, instructure.com, canvaslms.com, *.canvaslms.com, *.cluster95.canvas-user-content.com	Jun 2, 2025 – Jul 1, 2026	RSA 2048-bit	cluster95.canvas-user-content.com → Amazon RSA 2048 M03 → Amazon Root CA 1	SHA256withRSA	TLS_AES_128_GCM_SHA256 (GCM mode)	SHA-256	C and I	Cert Transparency enabled; forward secrecy supported; A+ overall
Subject: discord.com **CN:** discord.com **SANs:** discord.com, *.discord.com	Sep 8, 2025 – Dec 7, 2025	EC 256-bit, RSA 2048-bit	discord.com → WR1 → GTS Root R1	SHA384withECDSA	AES-128, AES-256, or ChaCha20-Poly1305	SHA-256	C and I	Uses elliptic curves; HSTS enabled; A+ overall
Subject: 4chan.org **CN:** 4chan.org **SANs:** 4chan.org, *.4chan.org	Sep 14, 2025 – Dec 13, 2025	RSA 2048-bit	4chan.org → WR1 → GTS Root R1	SHA256withRSA	AES-128-GCM, AES-256-GCM, ChaCha20-Poly1305	SHA-256	C and I (no forced secrecy for legacy clients)	Supports TLS 1.0/1.1; allows weak ciphers; grade B overall
Subject: eastman.com **CN:** eastman.com **SANs:** eastman.com, www.eastman.com, preview.eastman.com, recreation.eastman.com	Jul 28, 2025 – Aug 28, 2026	RSA 2048-bit	eastman.com → GeoTrust TLS RSA G1	SHA256withRSA	AES-128-GCM, AES-256-GCM, ChaCha20-Poly1305	SHA-256	C and I	Intermediate cert also signed to eastman.com; TLS 1.0/1.1 disabled; A+ overall

Subject: apple.com **CN:** apple.com **SANs:** apple.com	Sep 22, 2025 – Dec 17, 2025	RSA 2048 -bit	apple.com → Apple Public EV Server ECC CA 1-G1 → DigiCert Global Root G3	SHA256withRSA, SHA256withECDSA	AES-128/256-GCM, ChaCha20-Poly1305	SHA-256	C and I	Only A overall; HSTS not enforced; owns its own CA
Subject: *.tata-daewoo.com **CN:** *.tata-daewoo.com **SANs:** *.tata-daewoo.com, tata-daewoo.com	Oct 8, 2024 – Oct 28, 2025	RSA 2048 -bit	*.tata-daewoo.com → Sectigo RSA Domain Validation Secure Server CA → USERTrust RSA CA → AAA Cert Services	SHA256withRSA	AES-128/256-GCM, ChaCha20-Poly1305, AES-CCM, AES-CBC, 3DES, RC4, NULL	SHA-256, SHA-384 (in some GCM suites)	NONE	F grade; supports broken RC4/MD5; legacy cipher fallback
Subject: www.sweetwater.com **CN:** www.sweetwater.com **SANs:** www.sweetwater.com, sweetwater.com	Sep 9, 2025 – Sep 24, 2026	RSA 2048 -bit	www.sweetwater.com → DigiCert EV RSA CA G2 → DigiCert Global Root G2	SHA256withRSA	AES-128/256-GCM, ChaCha20-Poly1305, AES-CBC	SHA-256	C and I	TLS 1.3 not supported; A- overall; Cert 2 missing SNI data
Subject: coolmathgames.com **CN:** coolmathgames.com **SANs:** *.coolmathgames.com, coolmathgames.com	Oct 16, 2025 – Jan 14, 2026	RSA 2048 -bit, EC 256-bit	coolmathgames.com → R13 / E8	SHA256withRSA, SHA384withECDSA	AES-128/256-GCM, ChaCha20-Poly1305	SHA-256, SHA-384	C and I	Supports TLS_Fallback_SCSV ; TLS 1.3 enabled; grade B overall
Subject: *.temu.com **CN:** *.temu.com **SANs:** *.temu.com, temu.com	Jul 13, 2025 – Aug 14, 2026	RSA 2048 -bit	*.temu.com → GoDaddy Secure CA - G2	SHA256withRSA	AES-128/256-GCM, ChaCha20-Poly1305	SHA-256, SHA-384	C and I	A+ overall; strong TLS 1.3 setup; HSTS enabled

Subject: skydaz.com.tr **CN:** skydaz.com.tr **SANs:** *.skydaz.com.tr, skydaz.com.tr	Oct 3, 2025 – Jan 1, 2026	RSA 2048 -bit	skydaz.com.tr → R12	SHA256withRSA	AES-128/256-GCM, ChaCha20-Poly1305	SHA-256, SHA-384	C and I	A+ overall; OCSP stapling disabled; 0-RTT disabled